G. H. RAISONI COLLEGE OF ENGINEERING & MANAGEMENT, PUNE.

Department of Computer Engineering

Final Year Project Synopsis
2022 - 2023

Group Id - AB03

Project Title

Vulnerable University

Project Option - HackKeen Cyber Private Limited

Internal Guide - Prof. Gayatri Bendre

Presented By -

Abhishek Birdawade - BCOA03

Srushti Deshpande - BCOB93

Vaibhav Wagh - BCOB111

Technical Keywords - Cyber Security, Security testing, Penetration testing, Bug hunting, API testing platform, Test hacking skills legally, Technical Vulnerabilities, IDOR, Authentication, Authorization, Security Misconfiguration, Vulnerable University.

Problem Statement - Cyber security is a vast field and immerging daily. With increasing digital theft and cyber criminals, we need security tester and practitioner to help us tackle the increasing problem. It is necessary for them to learn testing without violating cyber laws. The vulnerable web application will provide a platform to learn and test their skills in their own local environment.

Abstract - Identifying vulnerabilities and ensuring security functionality by security testing is a widely applied measure to evaluate and improve the security of software. Due to the openness of modern software-based systems, applying appropriate security testing techniques is of growing importance and essential to perform effective and efficient security testing. Therefore, an overview of actual security testing techniques is of high value both for researchers to evaluate and refine the techniques and for practitioners to apply and disseminate them.

For this purpose, it first summarizes the required background of testing and security engineering. Then, basics and recent developments of security testing techniques applied during the secure software development lifecycle, i.e., model-based security testing, code-based testing and static analysis, penetration testing and dynamic analysis, as well as security regression testing are discussed. Finally, the security testing techniques are illustrated by adopting them for an example three-tiered web-based business applications. All above mentioned phases are covered in this project. By utilizing the project, the users will be able to test their skills, learn new skills and audit real-world websites with ease.

Goals & Objectives:

1.To identify the threats in the system

2.To measure the potential vulnerabilities of the system

3.To help in detecting every possible security risk in the system

4.To help developers in fixing the security problems through coding

Names of Conferences/Journals where papers can be published:

- IEEE/ACM Conferences/Journal
- OWSAP Foundation Journal
- Nullcon Conferences

Literature Survey:

Sr. No	Date	Author	Title	Summary
1.	03/11/2015	Michael Felderer, Matthias Büchler, Martin Johns	Security Testing: A Survey	This chapter provided a broad overview of recent security testing techniques.
2.	10/03/2016	Min Wei, Shuaidong Zhang, Keecheon Kim	A security testing platform for Wireless Sensor Networks	The test results show that the platform is a feasible platform for assessing device security levels in WSNs.
3.	23/10/2021	Andrew Hahn, Daniel R. Sandoval, Raymond E. Fasano, Christopher Lamb	Automated Cyber Security Testing Platform for Industrial Control System.	A platform that incorporates these three components to provide the most accurate representation of actual NPP networks and controllers is developed in this paper

Plan of Project Execution:

Using GitHub for storing and sharing the code, as well as maintaining versions of code phases.